Available online at www.sciencedirect.com
ScienceDirect
Journal of Algebra 312 (2007) 218–227
JOURNAL OF Algebra
www.elsevier.com/locate/jalgebra

Reed–Muller codes, the fourth cohomology group of a finite group, and the β-invariant ☆

Geoffrey Mason

Department of Mathematics, University of California, Santa Cruz, CA 95064, USA

Received 25 January 2006

Available online 13 December 2006

Communicated by Susan Montgomery

Abstract

We introduce the β-invariant $b(\omega)$ attached to a 4-cohomology class $\omega \in H^4(G,\mathbb{Z})$, G a finite group. Roughly speaking, $b(\omega)$ keeps track of the restriction of ω to subgroups of G of order 2. If G is an elementary abelian 2-group, we observe that b defines a natural isomorphism from $H^4(G,\mathbb{Z})$ to the shortened third order Reed–Muller binary code. In general, restricting ω to elementary abelian 2-subgroups produces an array of Reed–Muller codewords which can be exploited. We give two main applications: (a) for many of the larger sporadic simple groups, the 2-part of $H^4(G,\mathbb{Z})$ lies in the *nilpotent radical* of the cohomology ring (Proposition 4.1); (b) up to gauge equivalence, the twisted quantum double $D^\omega(G)$ has a trivial β-invariant (in the sense of quasi-Hopf algebras) if, and only if, ω is a nilpotent element in the cohomology ring (Proposition 5.2).

1. Introduction

Let G be a finite group, and let $(C_1,\dots,C_h)$ be a fixed ordering of a set of representatives of the conjugacy classes of subgroups of G of order 2. Fix a nonnegative integer n. We are concerned here with the map

$$b : Z^n(G,\mathbb{Z}) \longrightarrow \bigoplus_{i=1}^{h} \mathrm{Res}^G_{C_i} Z^n(G,\mathbb{Z})$$

☆ Supported by a NSF grant and faculty research funds granted by the University of California at Santa Cruz.
E-mail address: gem@cats.ucsc.edu.

0021-8693/$ – see front matter
doi:10.1016/j.jalgebra.2006.10.036

and the corresponding map in cohomology, also denoted by b,

$$b: H^n(G,\mathbb{Z}) \longrightarrow \mathbb{F}_2^h, \qquad \omega \longmapsto \left(\mathrm{Res}^G_{C_1}\,\omega, \ldots, \mathrm{Res}^G_{C_n}\,\omega\right). \tag{1}$$

(Here and below, we usually do not differentiate between cocycles and the cohomology classes that they define.)

Our main interest is in the case $n = 4$, in which case we call the image $b(\omega) \in \mathbb{F}_2^h$ the β-*invariant* of ω. This case is related, via the isomorphism $H^4(G,\mathbb{Z}) \cong H^3(G,\mathbb{C}^*)$, to issues concerning the structure of the twisted quantum double $D^\eta(G)$. This is a quasi-Hopf algebra canonically associated to G and a given 3-cocycle $\eta \in Z^3(G,\mathbb{C}^*)$ [DPR]. Part of the data defining a quasi-Hopf algebra is its β-invariant, and we will see (Section 5) that it is determined up to coboundaries by the β-invariant of η. This leads to several applications of the results we obtain here to twisted quantum doubles and their representations, and to orbifold conformal field theory. Some of these are discussed in Section 5, however the main purpose of the present paper is to discuss the rôle that the β-invariant plays in the cohomology of G.

The first case to consider is that when G is an elementary abelian 2-group $E \cong \mathbb{Z}_2^l$. The main observation here is that if $2k \leqslant l+1$ then the b-image of $H^{2k}(E,\mathbb{Z})$ is precisely the shortened $(2k-1)$th Reed–Muller code $\mathcal{R}(2k-1,l)$. Moreover, in degree 4 we will see (Proposition 2.2) that b induces an *isomorphism*

$$b: H^4(E,\mathbb{Z}) \xrightarrow{\sim} \mathcal{R}(3,l). \tag{2}$$

Reed–Muller codes are a well known and highly studied class of binary codes [V,CV], and much is known about their weight distribution. Via the isomorphism (2), they provide combinatorial information about the restriction of cohomology to subgroups of order 2 in E. One sees immediately, for example, that elements in $H^4(E,\mathbb{Z})$ are *detected* by restriction to subgroups of order 2.

For a general group G, one can restrict cohomology to the elementary abelian 2-subgroups, so that to a given 4-cocycle on G there are attached several Reed–Muller codewords of various lengths. Conjugation in G implies consistency constraints which restrict the nature of the map b. We illustrate the situation for some sporadic simple groups in Section 4. For example, we show (Proposition 4.1) that the 2-torsion in $H^4(G,\mathbb{Z})$ is *nilpotent* in the sense that

$$H^4(G,\mathbb{Z})_2 \subseteq \mathrm{rad}\, H^*(M,\mathbb{Z}) \tag{3}$$

(rad refers to the *nilpotent radical* of the cohomology algebra) for the following sporadic simple groups:

$$M_{22}, M_{23}, McL, Ly, J_3, J_4, Th, Fi_{22}, Fi_{23}, Fi'_{24}, M.$$

Essentially, when the 2-rank is large enough (we will see that this means at least 4) and the number of classes of involutions h is small, the burden of consistency is so great that it can often only be met trivially—that is, the restriction of b to each elementary abelian 2-group is trivial. Because of this circumstance, our results are related to Quillen's theory [Q].

For several sporadic simple groups G of small 2-rank, it is known that restriction to elementary abelian 2-groups detects cohomology (cf. [AM]). Display (3) suggests that this will be more

difficult to prove, and more likely to be false, for the larger sporadic groups. One obvious possibility is that $H^4(G,\mathbb{Z}) = 0$. The case in which $H^i(G,\mathbb{Z}) = 0$, $1 \leqslant i \leqslant 4$ is itself is of some interest: according to results of Jim Milgram [AM], M_{23} enjoys these properties and is the only known group which does so. In [G], David Green shows that the *odd* part of the integral cohomology $H^*(J_4,\mathbb{Z})$ of the largest Janko group occurs in degrees 6 or higher. Thus, $H^4(J_4,\mathbb{Z})$ is contained in the radical of cohomology, and J_4 is a good candidate to join M_{23}. On the other hand, using more constructive techniques from orbifold theory, we will show elsewhere that in the case of the Monster, $H^4(M,\mathbb{Z})$ has a direct summand of order divisible by 12.

The paper is organized as follows: in Section 2 we discuss the map b and the connection with Reed–Muller codes; in Section 3 we give some general applications, while Section 4 is concerned with applications to the cohomology of sporadic simple groups. The final Section 5 deals with applications to twisted quantum doubles.

2. Group cohomology and Reed–Muller codes

Let E be an elementary abelian 2-group $E \cong \mathbb{Z}_2^l$ of rank $l \geqslant 1$. Although the cohomology of E is well known, for our purposes it will be useful to develop a particular point-of-view. Let $g_1,\dots,g_l$ be a set of generators for E, and let $\lambda_1,\dots,\lambda_l$ be the dual basis for $\hat{E} = \mathrm{Hom}(E,\mathbb{F}_2)$. One knows [AM] that

$$H^*(E,\mathbb{F}_2) = S[\lambda_1,\dots,\lambda_l], \tag{4}$$

the symmetric algebra on $\lambda_1,\dots,\lambda_l$.

From the short exact

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\mu} \mathbb{Z} \xrightarrow{\varphi} \mathbb{Z}_2 \longrightarrow 0,$$

μ being multiplication by 2, there is a long exact sequence in cohomology

$$\cdots \longrightarrow H^k(G,\mathbb{Z}) \xrightarrow{\mu^*} H^k(G,\mathbb{Z}) \xrightarrow{\varphi^*} H^k(G,\mathbb{Z}_2) \xrightarrow{\beta} H^{k+1}(G,\mathbb{Z}) \longrightarrow \cdots \tag{5}$$

where β (the Bockstein map) is the connecting homomorphism. Now let us take $G = E \cong \mathbb{Z}_2^l$. Then for an integer $k \geqslant 1$, there are maps

$$H^{2k-1}(E,\mathbb{Z}_2) \xrightarrow{\beta} H^{2k}(E,\mathbb{Z}) \xrightarrow{\varphi^*} H^{2k}(E,\mathbb{Z}_2) \tag{6}$$

where in (6), β is *surjective* and φ^* is *injective*.

The number of involutions in E is $h = 2^l - 1$, and we fix an ordering of the h subgroups of E of order 2. We may, and shall, define the map b in display (1) for coefficients $\mathbb{Z}_2$ as well as $\mathbb{Z}$. Thus,

$$b : H^*(E,\mathbf{k}) \longrightarrow \mathbb{F}_2^h, \qquad \omega \longmapsto (\dots,\omega_C,\dots)$$

where C ranges over the subgroups of order 2 with given ordering,

$$\omega_C = \begin{cases} 1 & \text{if } \operatorname{Res}^E_C \omega \text{ is nontrivial,} \\ 0 & \text{if } \operatorname{Res}^E_C \omega \text{ is trivial,} \end{cases}$$

and $\mathbf{k}$ is either $\mathbb{Z}$ or $\mathbb{Z}_2$.

We wish to describe the image of the sequence (6) under the map b. To this end we introduce the (shortened) rth order Reed–Muller code $\mathcal{R}(r,l)$ of length h (cf. [V,CV] for further details). Keeping previous notation, set $H_i = \ker \lambda_i$, $A_i = E \setminus H_i$, and for a nonempty subset $S \subseteq \{1,2,\ldots,l\}$ define $A_S = \bigcap_{s\in S} A_i$. We identify a subset T of nonidentity elements in E with its characteristic function $\chi(T)$ considered as an element in $\mathbb{F}_2^h$ in the usual way. That is

$$t\text{th coordinate of } \chi(T) = \begin{cases} 1 & \text{if } t \in T, \\ 0 & \text{if } t \notin T. \end{cases}$$

Using this identification, we set

$$\mathcal{R}(r,l) = \text{span of all } A_S \text{ with } 1 \leqslant |S| \leqslant r. \tag{7}$$

The usual (unshortened) Reed–Muller code [CV] is derived from $\mathcal{R}(r,l)$ by adding a 2^lth coordinate with entry 0 to all words, and adjoining the all 1s vector $(1,1,\ldots,1)$. Combinatorially it makes little difference which of the two codes one uses, but for us it is a bit more convenient to use the shortened version. Note that $\mathcal{R}(r,l) = \mathbb{F}_2^h$ for $r \geqslant l$, and there are natural embeddings $\mathcal{R}(r,l) \to \mathcal{R}(r+1,l)$. We now have

Proposition 2.1. *For $k \geqslant 1$ there is a commuting diagram in which all vertical maps b are* surjections*,*

$$\begin{array}{ccccc} H^{2k-1}(E,\mathbb{Z}_2) & \xrightarrow{\beta} & H^{2k}(E,\mathbb{Z}) & \xrightarrow{\varphi^*} & H^{2k}(E,\mathbb{Z}_2) \\ \downarrow b & & \downarrow b & & \downarrow b \\ \mathcal{R}(2k-1,l) & \xrightarrow{\text{id}} & \mathcal{R}(2k-1,l) & \longrightarrow & \mathcal{R}(2k,l). \end{array} \tag{8}$$

Proof. First we calculate the image under b of the canonical monomial basis of the algebra (4), which is easy. For indices $1 \leqslant i_1 < i_2 < \cdots < i_r \leqslant l$ and positive integers $e_1,\ldots,e_r$, we see that the b-image of $\lambda_{i_1}^{e_1}\ldots\lambda_{i_r}^{e_r}$ coincides with that of $\lambda_{i_1}\ldots\lambda_{i_r}$. Moreover,

$$b : \lambda_{i_1}\ldots\lambda_{i_r} \longmapsto \chi(A_{i_1}\cap\cdots\cap A_{i_r}). \tag{9}$$

The surjectivity of $b : H^k(E,\mathbb{Z}_2) \to \mathcal{R}(k,l)$ follows immediately from this and the definition (7) of the Reed–Muller codes.

As for the integral cohomology $H^{2k}(E,\mathbb{Z})$, note that the restriction of a class $\omega \in H^{2k-1}(E,\mathbb{Z}_2)$ to an order 2 subgroup C is nontrivial if, and only if, the Bockstein $\beta(\omega)$ restricts nontrivially to C. Because the Bockstein is a surjection, this says exactly that the b-image of $H^{2k}(E,\mathbb{Z})$ coincides with the b-image of $H^{2k-1}(E,\mathbb{Z}_2)$. The proposition follows immediately. □

In the special case of $\mathbb{Z}$-coefficients and $k = 2$ we can say a bit more:

Proposition 2.2. *b induces an* isomorphism

$$b : H^4(E, \mathbb{Z}) \xrightarrow{\cong} \mathcal{R}(3, l). \tag{10}$$

Proof. We already know from Proposition 2.1 that b is a surjection, so it is enough to check dimensions. First note [V,CV] that

$$\dim \mathcal{R}(3, l) = \binom{l}{1} + \binom{l}{2} + \binom{l}{3}.$$

Set $\Delta = \varphi^* \circ \beta$. Then Δ is a degree 1 derivation of $H^*(E, \mathbb{Z}_2)$ satisfying $\Delta \circ \Delta = 0$ and $\Delta(\lambda_i) = \lambda_i^2$. Now $H^4(E, \mathbb{Z}) \cong \ker(\Delta : H^3(E, \mathbb{Z}_2) \to H^4(E, \mathbb{Z}_2))$, and we can calculate that $\ker \Delta$ has a basis consisting of elements $\lambda_i^4, \lambda_i^2\lambda_j^2$ and $\lambda_i^2\lambda_j\lambda_k + \lambda_i\lambda_j^2\lambda_k + \lambda_i\lambda_j\lambda_k^2$ where $1 \leqslant i < j < k \leqslant l$. As a result, $\dim H^4(E, \mathbb{Z}) = \dim \mathcal{R}(3, l)$, and the proposition is proved. □

3. Some general applications

In this section we illustrate how Proposition 2.2 together with the combinatorial properties of Reed–Muller codes can be used to get information about $H^4(G, \mathbb{Z})$ for a finite group G. For future reference we list some of the basic properties of the Reed–Muller codes $\mathcal{R}(r, l)$ [V,CV]:

$$\text{(a)} \quad \text{min weight} = 2^{l-r}; \tag{11}$$

$$\text{(b)} \quad \text{all codewords have weight divisible by } 2^{\lceil l/r \rceil - 1}; \tag{12}$$

$$\text{(c)} \quad \text{if } r < l \text{ then all codewords have even weight.} \tag{13}$$

($\lceil l/r \rceil$ is the *least* integer *no smaller* than l/r.) Although (c) is a special case of (b), it is worth emphasizing because of its utility.

In what follows, we use the following definitions and notation: an elementary abelian 2-subgroup of G is *maximal* if it is a maximal element in the poset of elementary abelian 2-subgroups of G with respect to containment; the 2-*rank* of G is the maximum of the ranks of its elementary abelian 2-subgroups; a *central* subgroup (or involution) of order 2 is a subgroup (element) of order 2 contained in the center of a Sylow 2-subgroup; $H^k(G, \mathbb{Z})_2$ is the 2-torsion subgroup of $H^k(G, \mathbb{Z})$. If E is an elementary abelian 2-subgroup of G of rank l, we let b_E denote the composition

$$b \circ \operatorname{Res}_E^G : H^4(G, \mathbb{Z}) \longrightarrow \mathcal{R}(3, l).$$

A well-known result of Quillen [Q,QV] says that a cohomology class in $H^k(G, \mathbb{Z}_2)$ lies in the radical $\operatorname{rad} H(G, \mathbb{Z}_2)$ if its restriction to every elementary abelian 2-subgroup is trivial. Proposition 2.2 permits a refinement in low degrees.

Proposition 3.1. *Let* $\omega \in H^4(G, \mathbb{Z})_2$. *Then the following are equivalent*:

(a) $\omega \in \operatorname{rad} H(G, \mathbb{Z})$;
(b) $\operatorname{res}_C^G \omega = 0$ *for all order* 2 *subgroups* $C \subseteq G$.

Proof. The implication (a) $\Rightarrow$ (b) is obvious. Our task is to establish that (b) $\Rightarrow$ (a). To this end, let $E \subseteq G$ be any elementary abelian 2-subgroup. First assume that $G = E$. In this case (b) amounts to the assumption that $b(\omega) = 0$. But then $\omega = 0$ follows from Proposition 2.2, and (a) holds.

In general, this argument shows that from (b) we obtain the triviality of $\mathrm{Res}_E^G \omega$ for every such E, hence also $\mathrm{Res}_E^G \varphi^*(\omega) = 0$. By Quillen's Theorem, $\varphi^*(\omega) \in \mathrm{rad}\, H(G, \mathbb{Z}_2)$, so that there is an integer n satisfying

$$0 = \varphi^*(\omega)^n = \varphi^*(\omega^n).$$

So $\omega^n \in \ker \varphi^* = \mathrm{im}\, \mu^*$, whence $\omega^n = 2\tau$ for suitable cohomology class τ. Therefore (a) holds, and the proposition is proved. □

We need some more notation: $Z_1, \ldots, Z_c$, and $Y_1, \ldots, Y_d$ are respectively the distinct conjugacy classes of central and noncentral subgroups of order 2 in G. Let $B_1, \ldots, B_c$ be representatives of the central classes.

Lemma 3.2. *Assume that G has even order, and let $E \subseteq G$ be a maximal elementary abelian 2-subgroup. The following hold*:

(a) $c \equiv 1 \pmod 2$;
(b) $|E \cap Z_j| \equiv 1 \pmod 2$, $1 \leqslant j \leqslant c$;
(c) $|E \cap Y_j| \equiv 0 \pmod 2$, $1 \leqslant j \leqslant d$.

Proof. Let X be the set of all subgroups of G of order 2, and note that $|X|$ is *odd*. G acts on X by conjugation, and the Y_i and Z_j are the G-orbits of even, respectively odd cardinality. Hence $c \equiv |X| \pmod 2$, and part (a) follows. The proof of parts (b), (c) is similar. One considers the conjugation action of E on Y_i or Z_j, noting that the fixed-points are exactly $E \cap Y_i$ and $E \cap Z_j$, respectively. □

Proposition 3.3. *Assume that G has 2-rank at least 4, and let $\omega \in H^4(G, \mathbb{Z})$. Then there are an* odd *number of indices j for which* $\mathrm{Res}_{B_j}^G \omega = 0$.

Proof. Fix a maximal elementary abelian 2-subgroup $E \subseteq G$ of rank $l \geqslant 4$. We consider the codeword $b_E(\omega) \in \mathcal{R}(3, l)$, more precisely its (Hamming) weight $w(b_E(\omega))$, i.e. the number of nonzero coordinates. We may choose notation so that $\mathrm{Res}_{B_j}^G \omega = 0$ for $1 \leqslant j \leqslant m$ and $\mathrm{Res}_{B_j}^G \omega \neq 0$ for $m + 1 \leqslant j \leqslant c$. We have to show that m is odd. From Lemma 3.2(a) it follows that

$$w\big(b_E(\omega)\big) \equiv c - m \equiv 1 - m \pmod 2.$$

On the other hand, since $l \geqslant 4$ then (13) implies that

$$w\big(b_E(\omega)\big) \equiv 0 \pmod 2.$$

The proposition follows from these two congruences. □

We illustrate how these results may be used.

Corollary 3.4. *Suppose that G has 2-rank at least 4 and exactly one class of involutions. Then*

$$H^4(G,\mathbb{Z})_2 \subseteq \operatorname{rad} H(G,\mathbb{Z}).$$

Proof. Let $\omega \in H^4(G,\mathbb{Z})_2$. Since there is only one class of involutions, it follows from Proposition 3.3 that $\operatorname{Res}^G_C \omega = 0$ for all order 2 subgroups $C \subseteq G$. Application of Proposition 3.1 now completes the proof. □

Corollary 3.5. *Assume that every subgroup of order 2 in G is contained in a cyclic subgroup of order 4. Then*

$$\operatorname{Im}\bigl(\beta : H^3(G,\mathbb{Z}_2) \longrightarrow H^4(G,\mathbb{Z})_2\bigr) \subseteq \operatorname{rad} H^*(G,\mathbb{Z}).$$

Proof. Let $\omega \in H^3(G,\mathbb{Z}_2)$, with C any subgroup of order 2. Then $C \subseteq D \subseteq G$ with D cyclic of order 4. Since $\operatorname{Res}^D_C H^3(D,\mathbb{Z}_2) = 0$ then $\operatorname{Res}^G_C \omega = \operatorname{Res}^D_C \operatorname{Res}^G_D \omega = 0$. Since Bockstein commutes with restriction we conclude that $\operatorname{Res}^G_C \beta(\omega) = 0$ for all C, and the corollary follows from Proposition 3.1. □

Because of the long exact sequence (5), another way to state the conclusions of the last result is as follows: all elements of order 2 in $H^4(G,\mathbb{Z})$ lie in the radical.

Corollary 3.6. *Assume that G has 2-rank at least 4 and exactly two conjugacy classes of involutions. Let $E \subseteq G$ be a maximal elementary abelian 2-subgroup of rank $l \geqslant 3$. If $\omega \in H^4(G,\mathbb{Z})_2$ does* not *lie in rad $H^4(G,\mathbb{Z})$ then*

$$|Y_1 \cap E| \text{ is divisible by } 2^{\lceil l/3\rceil - 1} \text{ and is at least } 2^{l-3}.$$

Proof. Clearly $E \setminus \{1\}$ is the disjoint union of $E \cap Y_1$ and $E \cap Z_1$. Recalling the notation $B_1 \in Z_1$, then $\operatorname{Res}^G_{B_1} \omega = 0$ by Proposition 3.3. Then Proposition 3.1 shows that $\operatorname{Res}^G_C \omega \neq 0$ for every $C \in Y_1$. In other words, the Hamming weight of $b_E(\omega) \in \mathcal{R}(3,l)$ is equal to $|Y_1 \cap E|$. Now the corollary follows from (11) and (12). □

4. Application to sporadic simple groups

We continue the considerations of Section 3, but now taking G to be a sporadic simple group. Further information about these groups, including some facts that we use below, can either be found directly in the Atlas [A] or deduced from the information in it.

First consider the first Janko group J_1. A Sylow 2-subgroup T satisfies $T \cong \mathbb{Z}_2^3$ and there is a unique class of involutions. It can be checked from the information given in [AM, Chapter VIII] that $H^3(G,\mathbb{Z}_2) \cong H^4(G,\mathbb{Z}) \cong Z_2$. In each case the corresponding cohomology ring has *trivial* radical. This shows that the rank condition in Corollary 3.4 cannot be improved.

A number of the sporadic simple groups satisfy the assumptions of Corollary 3.5, so all elements of order 2 in $H^4(G,\mathbb{Z})$ lie in the radical in this case. The precise list is as follows: M_{11}, ON, M_{22}, M_{23}, M_{24}, McL, Ly, He, J_3, J_4, HN, Th, Co_2, Co_1, Suz, Fi'_{24}, M. In fact we have

Proposition 4.1. *The following sporadic simple groups satisfy the condition $H^4(G,\mathbb{Z})_2 \subseteq \operatorname{rad} H(G,\mathbb{Z})$:*

$$M_{22}, M_{23}, McL, Ly, J_3, J_4, Th, Fi_{22}, Fi_{23}, Fi'_{24}, M.$$

Proof. To begin with, M_{22}, M_{23}, McL, Ly, J_3 and Th all satisfy the assumptions of Corollary 3.4, so that result supplies us with the desired conclusion in these cases. Next consider the cases J_4, Fi'_{24} or M. These three groups have two particular properties in common: each has exactly two conjugacy classes of involutions, and each contains a subgroup of the shape $Z_2^{11}.M_{24}$ such that the normal elementary abelian 2-subgroup, call it E, contains 1771 central involutions and 276 noncentral involutions. By considering the restriction to E, Corollary 3.6 tells us that if $H^4(G,\mathbb{Z})_2$ is *not* contained in the radical then we must have $8|276$, a contradiction.

It remains to handle the two smaller Fischer groups, where the argument is similar but a bit more intricate. In both cases there are three classes of involutions. Now Fi_{23} has a subgroup $Z_2^{11}.M_{23}$, and one can calculate that the maximal normal elementary abelian 2-subgroup E contains the following number of elements from each of the three classes of involutions (they are all central): 1771, 253, 23. Note that $1771 \equiv 3 \pmod 8$, $253 \equiv 5 \pmod 8$, $23 \equiv 7 \pmod 8$. The same argument used to establish Corollary 3.6 shows that if $\omega \in H^4(G,\mathbb{Z})_2$ is *not* contained in the radical, and if there are N order 2 subgroups $C \subseteq E$ satisfying $\operatorname{Res}_C^G \omega \neq 0$, then N is a positive integer divisible by 8. The only possibility is $N = 2024$, this being the weight of a codeword in $\mathcal{R}(3,11)$. But then in the corresponding *unshortened* Reed–Muller code (which includes the all 1s vector), there is a codeword of weight 25. Since the minimum weight (11) still applies to the unshortened code, we have the desired contradiction. In the final case of Fi_{22} one looks at the subgroup $Z_2^{10}.M_{22}$, where the relevant orbits have lengths 770, 231, 22. We get a contradiction in the same way—details omitted. This completes the proof of the proposition. □

5. The β-invariant

In this section we assume familiarity with the twisted quantum double construction [DPR]. Let $\omega \in Z^3(G,\mathbb{C}^*)$ be a normalized 3-cocycle. The β-invariant of the twisted quantum double $D^\omega(G)$ is the element

$$\beta = \sum_{g\in G} \omega\big(g, g^{-1}, g\big) e(g) \bowtie 1$$

in $D^\omega(G)$. The next result was obtained in collaboration with S.-H. Ng.

Lemma 5.1. *ω is cohomologous to a 3-cocycle ω' satisfying*

$$\omega'\big(g, g^{-1}, g\big) = \begin{cases} \omega(g,g,g) & \text{if } g \text{ has order } 2, \\ 1 & \text{otherwise.} \end{cases}$$

Proof. For each $a \in G$ of order at least 3, choose exactly one element from the pair $\{a, a^{-1}\}$, and let A denote the resulting set of elements of G. Define a 2-cochain f as follows:

$$f(g,h) = \begin{cases} \omega(g, g^{-1}, g) & \text{if } g = h^{-1} \in A, \\ 1 & \text{otherwise.} \end{cases}$$

Then

$$\delta f\big(g, g^{-1}, g\big) = \frac{f(g^{-1}, g)}{f(g, g^{-1})} = \begin{cases} \omega(g^{-1}, g, g^{-1}) & \text{if } g^{-1} \in A, \\ \omega(g, g^{-1}, g)^{-1} & \text{if } g \in A, \\ 1 & \text{otherwise.} \end{cases}$$

Set $\omega' = \omega\delta f$. Using the identity $\omega(g, g^{-1}, g)\omega(g^{-1}, g, g^{-1}) = 1$, it follows easily that ω' has the desired properties. □

The β-invariant of $D^{\omega'}(G)$ is

$$\beta' = \sum_{g^2\neq 1} e(g) \bowtie 1 + \sum_{g^2=1} \omega'(g, g, g)e(g) \bowtie 1,$$

which is evidently determined by the map b. Indeed, we have $\omega'(g, g, g) = \pm 1$ for an involution g, and the upper sign is taken if, and only if, $\mathrm{Res}^G_{\langle g\rangle}\,\omega'$ is trivial. Using the isomorphism $H^3(G, \mathbb{C}^*) \cong H^4(G, \mathbb{Z})$ and the fact that twisted quantum doubles corresponding to cohomologous 3-cocycles are gauge equivalent, we obtain from Proposition 3.1 the following:

Proposition 5.2. *The following are equivalent for a* 3*-cocycle* $\omega \in Z^3(G, \mathbb{C}^*)$:

(a) $D^\omega(G)$ *is gauge equivalent to a twisted quantum double* $D^{\omega'}(G)$ *for which the* β*-invariant is the identity element*;
(b) *the* 2*-part of* ω *lies in* $\mathrm{rad}\, H(G, \mathbb{Z})$.

The deeper meaning of the nilpotence condition in this context remains unclear to the author.

The β-invariant appears in other contexts concerning the twisted quantum double (cf. [MN]). In particular, it coincides with the *trace element* [MN, Proposition 9.2]. The triviality of the β-invariant then implies [MN, Corollary 9.3] that the Frobenius–Schur indicator of a simple $D^\omega(G)$-module M is 1 or -1 precisely when M admits a nondegenerate $D^\omega(G)$-invariant symmetric (respectively skew-symmetric) bilinear form, just as in the case of group algebras. After Propositions 4.1 and 5.2 we know, for example, that this is the case for each of the sporadic groups listed in Proposition 4.1 and all choices of 3-cocycle.

Acknowledgment

We thank S.-H. Ng for permission to include Lemma 5.1, which was obtained in collaboration with him.

References

[A] J. Conway, R. Curtis, S. Norton, R. Parker, R. Wilson, Atlas of Finite Groups, Clarendon Press, Oxford, 1985.
[AM] A. Adem, J. Milgram, Cohomology of Finite Groups, second ed., Grundlehren Math. Wiss., Springer-Verlag, Berlin, 2004.
[CV] P. Cameron, J. van Lint, Graph Theory, Coding Theory and Block Designs, London Math. Soc. Lecture Note Ser., vol. 19, Cambridge Univ. Press, Cambridge, 1975.
[DPR] R. Dijkgraaf, V. Pasquier, P. Roche, Quasi-Hopf algebras, group cohomology and orbifold models, in: Integrable Systems and Quantum Groups, World Scientific, River Edge, NJ, 1992.
[G] D. Green, On the cohomology of the sporadic simple group J_4, Math. Proc. Cambridge Philos. Soc. 113 (1993) 253–266.
[MN] G. Mason, S.-H. Ng, Central invariants and Frobenius–Schur indicators for semisimple quasi-Hopf algebras, Adv. Math. 190 (2005) 161–195.

[Q] D. Quillen, The spectrum of an equivariant cohomology ring, I, Ann. of Math. 94 (1971) 549–572;
D. Quillen, The spectrum of an equivariant cohomology ring, II, Ann. of Math. 94 (1971) 573–602.
[QV] D. Quillen, B. Venkov, Cohomology of finite groups and elementary abelian subgroups, Topology 11 (1972) 317–318.
[V] J. van Lint, Coding Theory, Lecture Notes in Math., vol. 201, Springer-Verlag, Berlin, 1971.